					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII07					Título del documento: **Política de Evaluación de Riesgos de Privacidad y EIPD (DPIA)**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos

Norma / Reglamento	Cláusula / Control / Artículo	Aplicabilidad	Tipo de cobertura	Comentario
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Riesgos y oportunidades del PIMS
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Evaluación de riesgos de privacidad
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Tratamiento de riesgos de privacidad y vinculación con la SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Cambios planificados del PIMS y reevaluación de riesgos
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Información documentada sobre riesgos de privacidad y EIPD (DPIA)
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Planificación y control operacional
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Evaluación operacional de riesgos de privacidad
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Tratamiento operacional de riesgos de privacidad
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Supervisión y medición de riesgos de privacidad
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Revisión por la dirección de riesgos de privacidad
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	No conformidad y acción correctiva relacionadas con riesgos

ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Evaluación de impacto en la privacidad
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Registros de tratamiento que respaldan la evaluación de riesgos
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Acuerdo con el cliente del encargado del tratamiento y asistencia en EIPD (DPIA)
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Información del encargado del tratamiento que respalda el cumplimiento del cliente
GDPR	Article 5(2)	Controller	Supporting	Evidencia de responsabilidad proactiva
GDPR	Article 24	Controller	Supporting	Responsabilidad y medidas del responsable del tratamiento
GDPR	Article 25	Controller	Supporting	Protección de datos desde el diseño y por defecto
GDPR	Article 28	Both	Supporting	Asistencia e instrucciones del encargado del tratamiento
GDPR	Article 30	Both	Supporting	Registros de tratamiento que respaldan la EIPD (DPIA)
GDPR	Article 32	Both	Supporting	Riesgo de seguridad y salvaguardas
GDPR	Article 35	Controller	Primary	Evaluación de impacto relativa a la protección de datos
GDPR	Article 36	Controller	Primary	Consulta previa

GDPR	Article 39	Conditional	Supporting	Asesoramiento del DPO y supervisión cuando corresponda
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Controles de privacidad, seguridad de la información y cumplimiento de privacidad
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Alcance, beneficios, criterio de activación y preparación de la PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Programa de protección de PII e identificación de requisitos
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Integración de la gestión organizativa de riesgos de privacidad

1. Alcance

1.1 Esta política define los requisitos para la evaluación de riesgos de privacidad, la evaluación preliminar de EIPD (DPIA), la ejecución de la EIPD completa, el tratamiento de riesgos, la aceptación del riesgo residual, la consulta, la revisión y la gestión de evidencias para el tratamiento de PII dentro del alcance del PIMS.

1.2 Esta política se aplica a lo siguiente:

1.2.1 actividades de tratamiento de PII nuevas y modificadas de forma material;

1.2.2 contextos de tratamiento como responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado;

1.2.3 sistemas, aplicaciones, servicios, procesos de negocio, proveedores, encargados del tratamiento, subencargados, transferencias internacionales y acuerdos de intercambio de datos que afecten al tratamiento de PII;

1.2.4 evidencias de riesgos de privacidad y EIPD (DPIA) mantenidas en REG04 y evidencias de apoyo mantenidas en REG02, REG03, REG08, REG09, REG10, REG11 y REG12.

1.3 Esta política no sustituye los controles del inventario de tratamientos, los controles de avisos de privacidad, los controles de consentimiento, los controles de derechos de los interesados, los controles de privacidad desde el diseño, los controles de proveedores, los controles de transferencias internacionales, los controles de seguridad de PII, los controles de incidentes, los controles de información documentada ni los controles de supervisión/auditoría/mejora. Esos requisitos se definen en las políticas relacionadas enumeradas en la sección 12.

1.4 A efectos de esta política, evaluación de riesgos de privacidad significa la identificación, análisis, evaluación, tratamiento, revisión y supervisión documentados de los posibles impactos adversos sobre la privacidad derivados del tratamiento de PII.

1.5 A efectos de esta política, DPIA significa una evaluación documentada utilizada para el tratamiento realizado por el responsable del tratamiento que probablemente entrañe un alto riesgo para los interesados y que evalúa la necesidad del tratamiento, la proporcionalidad, los riesgos, las salvaguardas, el riesgo residual, las necesidades de consulta y las condiciones de aprobación.

1.6 A efectos de esta política, alto riesgo residual de privacidad significa un riesgo de privacidad que permanece por encima del umbral de aceptación aprobado tras el tratamiento de riesgos propuesto o implementado.

1.7 A efectos de esta política, un cambio material significa cualquier cambio que afecte al alcance del PIMS, la finalidad del tratamiento, la base jurídica, las categorías de PII, las categorías de interesados, la escala del tratamiento, la tecnología de tratamiento, la supervisión o la elaboración de perfiles, la toma de decisiones automatizada, los interesados vulnerables, los destinatarios, los encargados del tratamiento, los subencargados, las transferencias internacionales, la conservación, los controles de seguridad, el perfil de riesgo, las instrucciones del cliente o el alcance de certificación.

2. Finalidad

2.1 La finalidad de esta política es asegurar que los riesgos de privacidad y las obligaciones de EIPD (DPIA) se identifiquen, evalúen, traten, aprueben, revisen y evidencien antes de que el tratamiento de PII genere un riesgo inaceptable para los interesados o para el PIMS.

2.2 Esta política permite a la organización demostrar una gobernanza de privacidad basada en riesgos, la responsabilidad proactiva del responsable del tratamiento respecto de la EIPD (DPIA), la asistencia del encargado del tratamiento en EIPD (DPIA), el tratamiento de riesgos documentado, la aprobación del riesgo residual, la toma de decisiones sobre consulta previa y la mejora continua de los controles de privacidad.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 definir criterios obligatorios de activación para la evaluación preliminar de riesgos de privacidad;

3.1.2 definir cuándo se requiere una EIPD completa;

3.1.3 asegurar que las decisiones del responsable del tratamiento sobre EIPD (DPIA) estén documentadas y sean revisables;

3.1.4 asegurar que la asistencia en EIPD (DPIA) por parte del encargado del tratamiento y del subencargado esté documentada cuando lo exijan la instrucción del cliente o el acuerdo;

3.1.5 asegurar que los riesgos de privacidad se evalúen antes de que avance un tratamiento de PII nuevo o modificado de forma material;

3.1.6 asegurar que los tratamientos de riesgos de privacidad se asignen, implementen y verifiquen;

3.1.7 asegurar que los altos riesgos residuales de privacidad se escalen y aprueben antes de que el tratamiento comience o continúe;

3.1.8 asegurar que las decisiones de consulta previa se documenten cuando persista un alto riesgo residual;

3.1.9 asegurar que las evidencias de riesgos de privacidad y EIPD (DPIA) se mantengan en REG04 y se vinculen con los objetos de evidencia relacionados;

3.1.10 evitar la creación de registros separados de EIPD (DPIA), riesgos o consulta fuera de REG04.

4. Declaraciones de la política

4.1 Evaluación preliminar de riesgos de privacidad

4.1.1 [Both] The Process Owner / Business Owner DEBE iniciar la evaluación preliminar de riesgos de privacidad en REG04 antes de que comience el tratamiento de PII nuevo o modificado de forma material registrado en REG02.

4.1.2 [Both] The Privacy Lead / PIMS Manager DEBE mantener los criterios de evaluación preliminar de riesgos de privacidad en REG04 antes de la operación inicial del PIMS y anualmente a partir de entonces.

4.1.3 [Controller] The Process Owner / Business Owner DEBE completar la evaluación preliminar de EIPD (DPIA) en REG04 antes de que comience el tratamiento por el responsable del tratamiento que cumpla los criterios de evaluación preliminar de riesgos de privacidad.

4.1.4 [Processor] The Vendor / Procurement Owner DEBE registrar los requisitos de asistencia en EIPD (DPIA) del cliente en REG08 antes de que comience el tratamiento por el encargado del tratamiento cuando el acuerdo con el cliente o la instrucción documentada exijan apoyo para la EIPD (DPIA).

4.1.5 [Both] The System Owner / Application Owner DEBE proporcionar evidencias de diseño del sistema, acceso, seguridad, registro de eventos y flujo de datos en REG04 antes de la aprobación de la evaluación de riesgos de privacidad para sistemas nuevos o modificados de forma material que traten PII.

4.1.6 [Both] The Privacy Lead / PIMS Manager DEBE registrar el resultado de la evaluación preliminar y la justificación de la decisión sobre la EIPD completa en REG04 antes de que avance la actividad de tratamiento.

4.2 Criterios de activación de EIPD (DPIA) y determinación de requisitos

4.2.1 [Controller] The Privacy Lead / PIMS Manager DEBE exigir una EIPD completa en REG04 antes de que comience un tratamiento por el responsable del tratamiento que probablemente entrañe un alto riesgo.

4.2.2 [Controller] The Process Owner / Business Owner DEBE remitir al Privacy Lead / PIMS Manager en REG04, antes de que comience el tratamiento, los tratamientos que impliquen gran escala, supervisión sistemática, elaboración de perfiles, decisiones automatizadas, categorías especiales de PII, datos sobre condenas penales o infracciones, interesados vulnerables, tecnología innovadora o tratamientos modificados de forma material.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor DEBE registrar su asesoramiento en REG04 antes de la aprobación de una decisión sobre el requisito de EIPD completa para tratamientos de alto riesgo realizados por el responsable del tratamiento.

4.2.4 [Both] The Process Owner / Business Owner DEBE reevaluar preliminarmente el riesgo de privacidad en REG04 antes de utilizar PII para una nueva finalidad, añadir un nuevo destinatario, introducir un nuevo encargado del tratamiento o subencargado, cambiar la arquitectura del sistema o iniciar una nueva transferencia internacional.

4.2.5 [Processor] The Privacy Lead / PIMS Manager DEBE documentar si se requiere apoyo del encargado del tratamiento para la EIPD (DPIA) en REG08 en un plazo de 10 días hábiles desde la recepción de una solicitud de asistencia en EIPD (DPIA) del cliente.

4.2.6 [Subprocessor] The Vendor / Procurement Owner DEBE documentar los requisitos de asistencia en EIPD (DPIA) del nivel superior en REG08 antes de que comience el subtratamiento cuando el acuerdo con el cliente del nivel superior o el encargado del tratamiento exija dicha asistencia.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Excepciones

9.1 Excepciones de riesgos de privacidad y EIPD (DPIA)

9.1.1 [All] The Process Owner / Business Owner DEBE solicitar cualquier excepción a esta política en REG12 antes de que se produzca la desviación.

9.1.2 [All] The Privacy Lead / PIMS Manager DEBE evaluar el impacto sobre la privacidad, legal, de certificación, operativo y para los interesados de cada excepción solicitada en REG04 o REG12 en un plazo de 10 días hábiles desde la solicitud.

9.1.3 [All] The Data Protection Officer / Privacy Advisor DEBE registrar su asesoramiento en REG12 antes de la aprobación de cualquier excepción que afecte a tratamientos de alto riesgo, finalización de EIPD completa, consulta previa, alto riesgo residual de privacidad o asistencia en EIPD (DPIA) del cliente.

9.1.4 [All] Top Management DEBE aprobar en REG12 las excepciones de riesgos de privacidad o EIPD (DPIA) que afecten a tratamientos de alto riesgo, alcance de certificación, consulta previa o altos riesgos residuales de privacidad no resueltos antes de que la excepción surta efecto.

9.1.5 [All] The Privacy Lead / PIMS Manager DEBE establecer en REG12 una fecha de caducidad no superior a 90 días para cada excepción aprobada de riesgos de privacidad o EIPD (DPIA) antes de su aprobación.

9.1.6 [All] The Process Owner / Business Owner DEBE cerrar o reevaluar cada excepción de riesgos de privacidad o EIPD (DPIA) en REG12 en un plazo de cinco días hábiles desde su vencimiento.

10. Aplicación

10.1 Aplicación de riesgos de privacidad y EIPD (DPIA)

10.1.1 [All] The Privacy Lead / PIMS Manager DEBE registrar como no conformidad en REG12 las evidencias de riesgos de privacidad o EIPD (DPIA) en REG04 que falten, sean inexactas, incompletas, estén vencidas o no estén aprobadas, en un plazo de cinco días hábiles desde su identificación.

10.1.2 [Controller] The Process Owner / Business Owner DEBE suspender los nuevos tratamientos de alto riesgo por el responsable del tratamiento cuando falten antes del lanzamiento las evidencias requeridas de aprobación de EIPD (DPIA) en REG04.

10.1.3 [Both] The System Owner / Application Owner DEBE bloquear la entrada en producción de sistemas que traten PII cuando falten antes de la aprobación de entrada en producción las evidencias requeridas de tratamiento de riesgos en REG04.

10.1.4 [Both] The Vendor / Procurement Owner DEBE bloquear la incorporación de proveedores, encargados del tratamiento, subencargados o acuerdos de intercambio de datos cuando falten antes de la aprobación del acuerdo las evidencias requeridas de riesgos de privacidad o asistencia en EIPD (DPIA) en REG04.

10.1.5 [All] Top Management DEBE revisar las no conformidades importantes de riesgos de privacidad o EIPD (DPIA) no resueltas en REG12 durante la revisión por la dirección.

10.1.6 [All] The Privacy Lead / PIMS Manager DEBE escalar los incumplimientos repetidos de plazos de evaluación preliminar, revisión de EIPD (DPIA) o tratamiento de riesgos de REG04 a Top Management en REG12 en un plazo de cinco días hábiles tras la segunda ocurrencia en un período de 12 meses.

10.1.7 [All] The Internal Audit / Compliance Reviewer DEBE verificar la eficacia de las acciones correctivas para no conformidades de riesgos de privacidad y EIPD (DPIA) en REG12 en la siguiente auditoría programada o en un plazo de 60 días desde el cierre, lo que ocurra primero.

11. Revisión y mantenimiento

11.1 Revisión y mantenimiento de la política

11.1.1 [All] The Privacy Lead / PIMS Manager DEBE revisar esta política en REG12 anualmente y en un plazo de 30 días desde un cambio material en los requisitos de riesgos de privacidad, EIPD (DPIA), consulta previa, asistencia del encargado del tratamiento o certificación.

11.1.2 [All] The Privacy Lead / PIMS Manager DEBE revisar anualmente en REG12 los criterios de evaluación preliminar de REG04, los criterios de activación de EIPD (DPIA), los criterios de calificación del riesgo y los criterios de aceptación del riesgo residual.

11.1.3 [All] The Data Protection Officer / Privacy Advisor DEBE revisar en REG12 los cambios significativos para la privacidad en esta política antes de su aprobación.

11.1.4 [All] Top Management DEBE aprobar los cambios materiales de esta política en REG12 antes de su publicación.

11.1.5 [All] The Privacy Lead / PIMS Manager DEBE actualizar REG03 y REG04 en un plazo de 15 días hábiles tras los cambios aprobados de la política que alteren la aplicabilidad de los controles, los criterios de riesgo o los requisitos de evaluación preliminar de EIPD (DPIA).

11.1.6 [All] The Privacy Lead / PIMS Manager DEBE registrar la comunicación de los cambios aprobados de esta política en REG11 en un plazo de 30 días desde su publicación.

12. Políticas relacionadas

12.1 Esta política está respaldada por las siguientes políticas relacionadas:

12.2 PII01 - Política del Sistema de Gestión de la Privacidad de la Información

12.3 PII02 - Política de Roles, Responsabilidades y Responsabilidad Proactiva de Privacidad

12.4 PII03 - Política de Inventario de Tratamientos de PII y Base Jurídica

12.5 PII04 - Política de Aviso de Privacidad y Transparencia

12.6 PII05 - Política de Gestión del Consentimiento y las Preferencias

12.7 PII06 - Política de Gestión de Derechos de los Interesados

12.8 PII08 - Política de Privacidad desde el Diseño y por Defecto

12.9 PII09 - Política de Recogida, Uso, Comunicación e Intercambio de PII

12.10 PII10 - Política de Conservación, Supresión y Eliminación de PII

12.11 PII11 - Política de Exactitud y Calidad de PII

12.12 PII12 - Política de Gestión de Privacidad de Encargados del Tratamiento, Subencargados y Terceros

12.13 PII13 - Política de Transferencias Internacionales de PII

12.14 PII14 - Política de Seguridad y Control de Acceso de PII

12.15 PII15 - Política de Gestión de Incidentes y Brechas de PII

12.16 PII17 - Política de Gestión de Información Documentada y Evidencias del PIMS

12.17 PII18 - Política de Supervisión, Auditoría y Mejora del PIMS

13. Normas y marcos de referencia

13.1 Esta política está mapeada con las siguientes normas y reglamentos. El mapeo explica cómo la política respalda los requisitos citados e identifica las cláusulas internas que los implementan o respaldan.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Mapeada a la identificación y planificación de acciones para riesgos y oportunidades de privacidad mediante criterios de evaluación preliminar, umbrales de riesgo, escalado y entradas para la revisión por la dirección. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Mapeada a la realización de la evaluación preliminar de riesgos de privacidad, la evaluación de riesgos de privacidad, la calificación del riesgo, la reevaluación y la evaluación de criterios de activación de EIPD (DPIA) antes de que avance un tratamiento nuevo o modificado de forma material. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Mapeada a la planificación del tratamiento de riesgos de privacidad, las actualizaciones de aplicabilidad de controles, la implementación del tratamiento, la aceptación del riesgo residual y la vinculación con la SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Mapeada a cambios planificados del PIMS y del tratamiento que desencadenan la reevaluación de riesgos de privacidad y la revisión de EIPD (DPIA). Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mapeada a información documentada controlada para evaluación preliminar de riesgos de privacidad, evidencias de EIPD (DPIA), tratamiento de riesgos, aceptación del riesgo residual, decisiones de consulta previa, excepciones, no conformidades y evidencias de revisión de políticas. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Mapeada a la operación de controles de riesgos de privacidad y EIPD (DPIA) antes de la entrada en producción, la incorporación, la aprobación del tratamiento, el cierre del tratamiento y la vinculación con acciones correctivas. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Mapeada a la evaluación operacional de riesgos de privacidad para cambios nuevos, modificados, de sistema, de proveedor, de transferencia y derivados de incidentes. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Mapeada al tratamiento operacional de riesgos de privacidad, la asignación del tratamiento, la implementación del tratamiento, el escalado de tratamientos vencidos y la verificación de eficacia. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Mapeada a la supervisión y medición de la cobertura de evaluación preliminar, el estado de EIPD (DPIA), los riesgos abiertos, las acciones de tratamiento vencidas, las acciones de proveedores, las acciones de tratamiento de seguridad, las acciones de reevaluación por incidentes y los hallazgos de auditoría. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Mapeada a la revisión por la dirección de altos riesgos residuales de privacidad, acciones de tratamiento vencidas, estado de EIPD completas, decisiones de consulta previa y excepciones importantes de riesgos de privacidad. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mapeada a no conformidades de riesgos de privacidad y EIPD (DPIA), excepciones, apertura de acciones correctivas, escalado y verificación de eficacia. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Mapeada a la evaluación de la necesidad de realizar, y a la implementación cuando corresponda, una evaluación de impacto en la privacidad para tratamientos nuevos o modificados realizados por el responsable del tratamiento. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Mapeada a registros de tratamiento que respaldan las entradas de evaluación de riesgos de privacidad y EIPD (DPIA), incluidas la finalidad, las categorías, los sistemas, los destinatarios, las transferencias y los proveedores. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mapeada a acuerdos con clientes del encargado del tratamiento y obligaciones de asistencia en EIPD (DPIA) del cliente. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Mapeada a la provisión por el encargado del tratamiento de la información necesaria para el cumplimiento del cliente, incluida la asistencia en EIPD (DPIA) y las evidencias de apoyo al cliente. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeado a evidencias de responsabilidad proactiva para la evaluación preliminar de EIPD (DPIA), decisiones de EIPD completa, tratamiento de riesgos, aceptación del riesgo residual, decisiones de consulta previa, excepciones, hallazgos de auditoría y acciones correctivas. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Mapeado a la responsabilidad del responsable del tratamiento respecto de medidas adecuadas de riesgos de privacidad, revisión de riesgos residuales altos, aprobación por la dirección y mantenimiento de la política. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Mapeado a evidencias de privacidad desde el diseño y privacidad por defecto utilizadas en la evaluación de riesgos y antes de la aprobación de entrada en producción. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mapeado a asistencia en EIPD (DPIA) por encargados del tratamiento y subencargados, gestión de instrucciones del cliente y evidencias de tratamiento de riesgos de proveedores. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Mapeado a registros de tratamiento que respaldan las entradas de evaluación de riesgos de privacidad y EIPD (DPIA). Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mapeado a entradas de riesgos de seguridad de PII, selección de salvaguardas, tratamiento de riesgos de seguridad y actualizaciones del estado de controles de seguridad. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mapeado a la evaluación preliminar de EIPD (DPIA), la determinación del requisito de EIPD completa, el contenido de EIPD (DPIA), el asesoramiento del DPO, la revisión y el bloqueo de tratamientos de alto riesgo sin la aprobación requerida de EIPD (DPIA). Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Mapeado a la toma de decisiones de consulta previa, el asesoramiento del DPO, la aprobación de Top Management y las acciones de continuación, suspensión, rediseño o consulta cuando persista un alto riesgo residual. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mapeado al asesoramiento y supervisión del Data Protection Officer / Privacy Advisor cuando corresponda para decisiones de EIPD (DPIA), tratamientos de alto riesgo, consulta previa y cambios de política. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Mapeada a la identificación de controles de privacidad, salvaguardas de seguridad, cumplimiento de privacidad, evidencias de riesgos de privacidad, supervisión y revisión. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapeada al alcance del proceso de PIA, los beneficios, la determinación de criterios de activación, la preparación, las entradas de evaluación, las evidencias de partes interesadas y la estructura del informe de EIPD (DPIA) mantenida en REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Mapeada a requisitos del programa de protección de PII, identificación de requisitos de protección de PII, selección de controles basada en el riesgo y vinculación del tratamiento de riesgos de privacidad. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Mapeada a principios organizativos de riesgos de privacidad, liderazgo, integración, evaluación de riesgos, tratamiento de riesgos, supervisión y revisión, y registro e información. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].